一种基于辫群共轭的数字签名及其验证方法

技术领域

本发明涉及信息安全领域中一种基于辫群的共轭搜索（*CSP*）问题和共轭判定（*CDP*）问题间差异的数字签名及其验证方法(*ECSS*), 具体是签名者如何发布一个带有自己私钥签名文件以便验证者使用签名者的公钥来验证该文件是否为签名者发布的签名文件的方法。

背景技术

现目前广泛使用的数字签名技术是 *RSA* 签名体制，它的安全性是建立在大数分解的困难性上的，然而随着计算机处理能力的不断提高和相关的研究逐渐深入，*RSA* 不得不不断的加大模数 *n* 位数以确保安全性，从 512 比特到 1024 比特到 2048 比特。由于密钥的位数过长，导致产生大素数和指数计算的计算量都很大，因此 *RSA* 的效率不是很高；而如果为了提高效率采用硬件实现，则位数过长导致设备更复杂、成本更高，而且由于硬件实现方式的不可改性，硬件的使用寿命缩短，导致成本的进一步提高。

自从 2000 年韩国学者 *Ki Hyoung KO*、*Sang Jin Lee* 在 *CRYPTO 2000* 提出了一种基于辫群共轭问题的困难性的密钥交换协议和公钥加密体制以来（*K. H. Ko， S. J. Lee， J. H. Cheon， J. W. Han， J. S. Kang and C. S. Park， New Public-Key Crytosystem Using Braid Groups， Proc. of Crypto 2000， LNCS 1880， Springer-Verlag (2000) 166 183.*），辫群公钥密码体制得到了广泛的研究。然而它的数字签名体制一直没有一个很好的解决方案。直到 2003 年，韩国学者 *Ki Hyoung KO*、*Doo Ho Cho* 提出并实现了两种基于辫群共轭问题的签名体制（*Ki Hyoung Ko and Doo Ho Choi and Mi Sung Cho and Jang Won Lee New Signature Scheme Using Conjugacy Problem Cryptology ePrint Archive: Complete Contents 2003/168*）简单共轭签名体制 (*SCSS*)以及共轭签名体制 (*CSS*)。我们简要介绍 *SCSS* 以及 *CSS* 这两种签名体制。

简单共轭签名体制 *SCSS*:

公共参数: 辫群 B_n 散列函数 h

密钥生成：公钥：一个*CSP*问题为困难问题的共轭对（x，x'）$\in B_n \times B_n$，

私钥：$a \in B_n$，满足$x'=a^{-1}xa$；

签名：对于一个给定的比特串消息 M，M 的签名 $sign(M)=a^{-1}ya$，其中院 $y=h(M)$；

验证：一个签名 $sign(M)$是合法的，当且仅当：$sign(M)$与 y 共轭且$x'sign(M)$与 xy 共轭。

然而由于攻击者可以获得很多对的（ y_i ，$a^{-1}y_ia$ ），从而可能造成私钥 a 的秘密信息泄漏，即 *k-CSP* 问题。为了克服以上问题，他们提出了 *CSS* 签名体制。

共轭签名体制*CSS*:

公共参数：辫群 B_n 散列函数 h

密钥生成：公钥：一个*CSP*问题为困难问题的共轭对（x，x'）$\in B_n \times B_n$，

私钥：$a \in B_n$，满足$x'=a^{-1}xa$；

签名：对于一个给定的消息M，随机选择一个随机辫元$b \in B_n$，计算 $\alpha = b^{-1}xb$，$y=h(M\|\alpha)$，$\beta = b^{-1}yb$，$\gamma = b^{-1}aya^{-1}b$，消息M的签名$sign(M)=(\alpha, \beta, \gamma)$。

验证：消息 M 的签名 $sign(M)=(\alpha, \beta, \gamma)$为合法签名当且仅当满足：$\alpha \sim x, \beta \sim \gamma \sim y, \alpha\beta \sim xy, \alpha\gamma \sim x, y$。

CSS 签名体制由于引入了随机辫元 b，因此很好的克服了 *k-CSP* 问题。但是可以发现，由于增加了更多的计算和数据，因此整个效率明显下降。

发明内容

本发明的发明目的在于，为了克服了现有技术中针对因大数分解攻击以及产生大素数消耗计算资源过大，及 *CSS* 为解决 *SCSS* 中的 *k-CSP* 问题而增加更多的计算和数据而存在的产生密钥和签名验证时间过长的问题，提供一种基于辫群共轭问题的数字签名及验证方法，减少计算量和数据，提高整个签名体制的效率。

为实现上述的发明目的，本发明提供一种基于辫群共轭的数字签名方法，该方法涉及到的参数为：签名方 S，签名验证方 V，需要签名的消息 M，所需

的系统参数：辫群生成元个数 n，辫群左子群生成元个数 m，辫元长度上界 l，辫群 $B_n(l)$，$B_n(l)$的左子群 $LB_m(l)$，$B_n(l)$的右子群 $RB_{n-1-m}(l)$，从比特串{0，1}*到辫群 $B_n(l)$的单向散列函数 h；所述签名方法包括以下步骤：

步骤1、签名方S选择三个辫元 $x \in LB_m(l)$，$x' \in B_n(l)$，$a \in B_n(l)$，使得他们满足 $x' = a^{-1}xa$，且已知x和x'要找到a在计算上是不可行的，并将辫元对(x'，x)作为S的公钥，辫元a作为S的私钥；

步骤2、签名方S对需要签名的消息M使用散列函数h得到 $y=h(M) \in B_n(l)$；

步骤3、随机生成一个辫元 $b \in RB_{n-1-m}(l)$，然后使用自己的私钥a和产生的随机辫元b对消息M签名得到 $Sign(M) = a^{-1}byb^{-1}a$；

步骤4、签名方S将消息M以及M的签名Sign(M)输出。

其中，所述步骤1中S的公钥辫元对(x'，x)及私钥辫元a的生成包括以下步骤：

步骤 1a、选定系统参数辫群公钥对间的距离 d；

步骤 1b、将辫元 x 表示为标准形式 $x=\Delta^u \pi_1 \pi_2 \cdots \pi_l$；

步骤 1c、随机选择一个辫元 b 属于集合 $B_n(5\ l)$

步骤 1d、计算 $x'=b^{-1}xb, a=b$；

步骤1e、随机产生一个比特，如为1，计算 $x' = decycling(x'), a = a\ \pi_l$；否则，计算 $x'=cycling(x')$，$a = a\ \tau^u(\pi_1)$；

步骤1f、判断x'是否属于集合SSS(x)以及 $l(x') \leqslant d$是否都成立，若都成立输出（x, x'）为公钥，a为私钥；若有一个不成立，则执行步骤1e。

所述步骤 2 使用散列函数 h 得到 $y=h(M) \in B_n(l)$的处理过程包括以下步骤：

步骤 2a、择一个普通散列函数 H，其输出 $H(M)$长度为 $l\ [log(2,n!)]$，然后将 $H(M)$一次等分为 l 段 $R_1||R_2|| \cdots ||R_l$；

步骤 2b、将 Ri 对应为置换辫元 Ai，然后计算 $h(M) = A1*A2 \cdots Al$ 即为所求的 $h(M)$。

本发明还提供一种基于辫群共轭的数字签名的验证方法，其特征在于，包括以下步骤：

步骤 1、签名验证方 V 接收签名方 S 发送的信息 M 以及 M 的签名 $Sign(M)$

后，获取签名方 S 的公钥；

步骤 2、利用系统参数散列函数 h 对消息 M 进行计算，得到 $y=h(M)$；

步骤 3、判定 $sign(M)$ 与 y 是否共轭，若不共轭，则 $sign(M)$ 不是一个合法签名，验证失败；若共轭，则执行步骤 4；

步骤 4、利用已获取的 S 的公钥计算 $sign(M)$ x' 和 xy，并判定二者是否共轭，若不共轭，则 $sign(M)$ 不是一个合法签名，验证失败；若共轭，则 $sign(M)$ 为消息 M 的合法签名。

其中，所述步骤 1 中获取签名方 S 的公钥的方式为带外方式或接收由签名方 S 发送的公钥方式；所述步骤 3 中判定 $sign(M)$ 与 y 是否共轭和步骤 4 中判定 $sign(M)$ x' 和 xy 是否共轭采用算法 $BCDA$。

另外，本发明还提供一种基于辫群共轭的既包括签名方和验证方的数字签名及其验证方法（$ECSS$），该方法涉及到的参数为：签名方S，签名验证方V，需要签名的消息M，辫群生成元个数n，辫群左子群生成元个数m,辫元长度上界l,辫群 $B_n(l)$，

$B_n(l)$的左子群$LB_m(l)$，$B_n(l)$的右子群$RB_{n-1-m}(l)$，从比特串{0，1}*到辫群 $B_n(l)$ 的单向散列函数h；所述签名及其验证方法包括以下步骤：

步骤1、签名方S选择三个辫元$x \in LB_m(l)$，$x' \in B_n(l)$，$a \in B_n(l)$，使得他们满足$x' = a^{-1}xa$，且已知x和x'要找到a在计算上是不可行的，并将辫元对(x', x)作为S的公钥，辫元a作为S的私钥；

步骤2、签名方S对需要签名的消息M使用散列函数h得到$y=h(M) \in B_n(l)$；

步骤3、随机生成一个辫元$b \in RB_{n-1-m}(l)$，然后使用自己的私钥a和产生的随机辫元b对消息M签名得到$Sign(M) = a^{-1}byb^{-1}a$；

步骤 4、签名方 S 将消息 M 以及消息 M 的签名 $Sign(M)$发送给签名验证方 V；

步骤 5、签名验证方 V 接收签名方 S 发送的信息 M 以及 M 的签名 $Sign(M)$ 后，获取 S 的公钥；

步骤 6、利用系统参数散列函数 h 对消息 M 进行计算，得到 $y=h(M)$；

步骤 7、判定 $sign(M)$ 与 y 是否共轭，若不共轭，则 $sign(M)$ 不是一个合法签名，验证失败；若共轭，则执行步骤 8；

步骤 8、利用已获取的 S 的公钥计算 $sign(M)\,x'$ 和 xy，并判定二者是否共轭，若不共轭，则 $sign(M)$ 不是一个合法签名，验证失败；若共轭，则 $sign(M)$ 为消息 M 的合法签名。

从上述方案可知，本发明提供的数字签名及其验证方法有如下优点：

由于加入了随机辫元 b，使得针对每个消息 M，共轭对$(sign(M),\ h(M))$的共轭元为 $b^{-1}a$，由于 b 为随机因子，每次签名选择的 b 一般都不一样，因此每次的共轭元都不相同，从而掩盖了私钥 a 的信息泄漏，避免了在现有技术中 *SCSS* 签名体制中单一使用私钥 a 作为共轭对$(sign(M),\ h(M))$的共轭元的 *k-CSP* 问题。本发明提供的签名体制 *ECSS* 利用了辫群左子群和右子群之间的可交换性，直接加入一个随机辫元，用以保护密钥的秘密信息，提高签名算法的安全性。而 *CSS* 则依靠引入两个辅助辫元用以保护密钥秘密信息。*ECSS* 相对 *CSS* 最大的优点是在不降低安全性的基础上，减少了参与的辫元的数目和共轭判定的次数，从而大大提高了签名的运算效率，三种签名体制的比较具体参看表 1。

表 1

签名体制	签名计算量	验证计算量	签名数据量	安全性
SCSS	共轭计算：1 次 散列计算：1 次	共轭判定：2 次 散列计算：1 次 辫群运算：2 次	1 个辫元	存在 *k-CSP* 问题，安全性较低，基于 MCSP 问题
CSS	共轭计算：4 次 散列计算：1 次	共轭判定：5 次 散列计算：1 次 辫群运算：4 次	3 个辫元	引入随机化密钥因子，解决了 *k-CSP* 问题，基于 *MTSP* 问题
本发明方法（*ECSS*）	共轭计算：2 次 散列计算：1 次	共轭判定：2 次 散列计算：1 次 辫群运算：2 次	1 个辫元	引入随机化密钥因子，解决了 *k-CSP* 问题，基于 *MCSP* 问题。

本发明相对于传统的*RSA*签名方法使用完全不同体系的数学基础，不需要产生大素数，大大节省了密钥的位数和签字的位数，节约了计算资源，提高

了签名验证效率。在现有技术中给出的*CSS*签名方法在*Pentium III 866MHz*处理器上得到的数据如表2所示（其中，默认设置的参数l=3，d=4，$2^{31}<p<2^{32}$，r=3）：

表2

n	公钥位数	签名位数	密钥生成时间	签名时间	验证时间	安全强度
20	370	1653	17.82 ms	18.68 ms	30.87 ms	2^{220}
24	478	2138	21.70 ms	22.79 ms	41.75 ms	2^{356}
28	591	2648	24.42 ms	25.77 ms	59.59 ms	2^{530}

而本方法相对于*CSS*签名方法签名时间和验证时间都将大大减少，因此相对*RSA*有效率更高的优点。

附图说明

图 1 本发明基于辫群共轭的数字签名方法流程图；

图 2 为本发明基于辫群共轭的数字签名方法中的密钥生成流程图；

图 3 为本发明基于辫群共轭的数字签名方法中的单向散列函数 h 的处理流程图；

图 4 为本发明对基于辫群共轭的数字签名的验证流程图；

图 5 为本发明 *CDP* 问题判定算法 *BCDA* 处理流程图；

图 6 为本发明基于辫群共轭的既包括签名方和验证方的数字签名及其验证方法流程框图。

具体实施方式

由于本发明涉及到一系列的数学原理，首先将本发明的数学背景阐述如下：

辫群 B_n（n 为群参数）是由 *Artin* 生成元 σ_1，σ_2，……，σ_{n-1} 生成的有限表示的无限群，并且它的生成元 σ_1，σ_2 …… σ_{n-1} 满足以下关系：

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad (|i-j|>1, \quad 1<i, j<n) \qquad (1)$$

$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ $(|i-j|>1,\ 1<i, j<n)$ （2）

由左边m个生成员 σ_1， σ_2 …… σ_{m-1}生成的群叫B_n的左子群，记做LB_m；而由右边的$n-1-m$个生成元 σ_{m+1}， σ_{m+2} …… σ_{n-1}生成的子群叫B_n的右子群，记做RB_{n-1-m}。由生成元关系（1）显然可知：任取$(x, y) \in LB_m \times RB_{n-1-m}$，有$xy=yx$。对于一个辫元$b$，若他只包含$\sigma_1$， σ_2 …… σ_{n-1}而不含σ_1， σ_2 …… σ_{n-1}的逆元，则称b为一个正元。若对于正元b、a，有一个正元或单位元c使得$b=ac$，则称a为b的子元。辫元$\Delta=(\sigma_1\sigma_2\cdots\sigma_{n-1})(\sigma_1\sigma_2\cdots\sigma_{n-2})\cdots(\sigma_1\sigma_2)(\sigma_1)$称为辫群$B_n$的本元。$\Delta$满足$\Delta b = \tau(b)\Delta$， $\tau(\sigma_i)=\sigma_{n-i}$。其中$\Delta$的子元称作置换元，他们组成的集合和对称群$\Sigma$n的n!个元素一一对应。因此$\Delta$的子元可用一个置换$\pi$:{0， 1， ...， n－1} → {0， 1， ...， n－1}来表示。任何一个辫元b都存在唯一的一个标准表示形式：$b = \Delta^u\pi_1\pi_2\cdots\pi_l$，其中$\pi_i$为一个置换元。$b$的几个长度定义如下：$inf(b) = u$， $sup(b) = u + l$ ， $l(b) = l$。

在一个辫群 B_n 中，如果对于两个辫元 x，$y \in B_n$，存在一个辫元 $a \in B_n$ 使得 $y=a^{-1}xa$，则称辫元 x，y 共轭，记做 $x \sim y$，而辫元 a 称作共轭对（x，y）的共轭元，显然“~”是一种等价关系。辫群的基本共轭问题包括共轭判定问题 *CDP* 问题和共轭元搜索问题 *CSP* 问题。所谓 *CDP* 问题就是指：任意给出辫元对（x，y）$\in B_n \times B_n$，判断 $x \sim y$ 是否成立。根据群表示理论，对于任何群 G，总存在一个从 G 到某一个环的同态，该同态对共轭关系保持不变，因此 *CDP* 问题对于任何群在计算上总是可解决的。在现有的基于辫群共轭问题的签名体制中给出了一个算法可以在多项式时间内以任意高的概率解决 *CDP* 问题。所谓 *CSP* 问题就是指：对于一个给定的共轭辫元对（x，y）$\in B_n \times B_n$（$x \sim y$），找到一个辫元 $a \in B_n$，使得 $y=a^{-1}xa$。对于辫群的来说，目前不存在一个有效的算法可以在多项式时间内解决 *CSP* 问题，因此对随机选取的一共轭对（x，y）$\in B_n \times B_n$，他们的 *CSP* 问题将以很高的概率为一个困难问题。而本文提出的数字签名方法的安全性是建立在 *MCSP* 问题（匹配共轭搜索问题）的困难性上的，在现有的基于辫群共轭问题的签名体制中证明了 *MCSP* 问题与 *CSP* 问题的困难等价性。所谓 *MCSP* 问题对他的描述如下：

已知：辫群 B_n 的一个共轭对（x，x'）$\in B_n \times B_n$，和一个辫元 $y \in B_n$

问题：找到一个$y' \in B_n$满足：$y \sim y'$ $xy \sim x'y'$

以下通过附图对本发明所述的方法进行详细的说明:

所需公共参数: 辫群 B_n ， 左辫群 LB_m ，右辫群 RB_{n-1-m} ，散列函数 h，其中，B_n 的生成元为 $\sigma_1 \sigma_2 \cdots\cdots \sigma_{n-1}$，左辫群 LB_m 为生成元 σ_1，$\sigma_2 \cdots\cdots \sigma_{m-1}$ 生成的 B_n 的子群，右辫群 RB_{n-1-m} 为生成元 σ_{m+1}，$\sigma_{m+2} \cdots\cdots \sigma_{n-1}$ 生成的 B_n 的子群。

其公钥为一对 *CSP* 问题为困难问题的共轭对（x，x'）$\in LB_m \times B_n$，私钥为 $a \in B_n$，满足 $x' = a^{-1}xa$;

签名方对消息 M 签名的流程如图 1 所示，对于一个给定的消息 M，首先使用散列函数 h 计算得到 $y=h(M)$，使用算法 *PBG* 随机选取一个秘密随机辫元 $b \in RB_{n-1-m}$，计算 byb^{-1}，计算消息 M 的签名 $sign(M)=a^{-1}byb^{-1}a$，输签名方 S 将消息 M 以及 M 的签名 $Sign(M)$ 输出。

而对于一个攻击者来说，他要想伪造一个消息 M 的签名，所能知道的只包括公钥（x，x'），和 $y=h(M)$，要想伪造的签名 $sign(M)$ 满足 $sign(M) \sim y$、x' $sign(M) \sim xy$，显然等价于解决 *MCSP* 问题，因此是不能做到的。

而对于可以截获分析的消息签名对（y_i，$b^{-1}ay_ia^{-1}b$），由于加入了随机辫元 b，可以很好的避免 *k-CSP* 问题。所谓 *k-CSP* 问题描述如下:

已知: k 对共轭对（x_1，x_1'），……，（x_k，x_k'）$\in B_n \times B_n$ 且 $x_i' = a^{-1}x_ia$ $(i=1 \cdots k)$;

问题: 找到 $b \in B_n$，使得 $x_i' = b^{-1}x_ib$ $(i=1, 2 \cdots\cdots k)$。

其中，为了安全的产生密钥，先定义一些概念，对于一个辫元 $x \in B_n(l)$，定义他的 super summit 集 $SSS(x)=\{y \in B_n(l) \mid y \sim x, inf(y)=Maxinf(x), sup(y)=Minsup(x)\}$。整个签名算法的安全强度为 $|SSS(x)|$，约为 $\left(\frac{n}{4}\right)^{n(n-1)/2}$。若 $y \sim x$，定义 x、y 间的距 $d(x, y)=min\{l(b) \mid y=b^{-1}ab\}$，然后再定义 $s(x,d)=\{y \in SSS(x) \mid d(x,y) \le d\}$。选取 $x' \in s(x, d)$，则共轭对（x'，x）的 *CSP* 问题为困难问题，可以作为密钥。具体地，密钥生成的流程如图2所示，下面介绍算法 $RSSBG(x, d)=(x', a)$ 用以随机产生 $x' \in s(x, d)$ 且 $x' = a^{-1}xa$，从而得到安全公钥（x'，x）和私钥 a，也就是密钥生成的过程，具体过程如下:

步骤 11、选定系统参数辫群公钥对间的距离 d;

步骤 12、将辫元 x 表示为标准形式 $x=\Delta^u \pi_1 \pi_2 \cdots \pi_l$;

步骤 13、随机选择一个辫元 b 属于集合 $B_n(5l)$;

步骤 14、计算 $x'=b^{-1}xb, a=b$;

步骤 15、随机产生一个比特，如为 1，则计算 $x'=decycling(x'), a=a\,\pi_l$; 否则，计算 $x'=cycling(x')$，$a=a\,\tau^u(\pi_l)$;

步骤16、判断x'是否属于集合$SSS(x)$以及 $l(x')\leqslant d$是否都成立，若都成立输出（x, x'）为公钥，a为私钥；若有一个不成立，则执行步骤15。

使用散列函数h计算得到$y=h(M)$，其流程如图3所示：

对于一个从比特串{0，1}*到辫群$B_n(l)$的散列函数h，首先使用一个普通散列函数将{0，1}*压缩得到固定长度的比特串{0，1}^{N}，其中$N=l[\log_2 n!]$。然后将{0，1}^{N}分为l段$r_1\|r_2\|\cdots\|r_l$，每一段的长度都为$[\log_2 n!]$。由于$B_n(l)$的置换元有$n!$个，故可在置换元和整数集$[0, n!-1]$间建立一个一一映射，再依次将r_k转化为[0，n!-1]间某一个整数，再将这个整数转化为与其相对应的置换元P_k，最后得到$h(M)=\prod_{k=1}^{l} P_k$。

本发明对基于辫群共轭的数字签名的验证流程如图4所示，包括以下步骤：

步骤 20、签名验证方 V 接收签名方 S 发送的信息 M 以及 M 的签名 $Sign(M)$ 后，获取 S 的公钥；

步骤 21、利用系统参数散列函数 h 对消息 M 进行计算，得到 $y=h(M)$;

步骤 22、判定 $sign(M)$ 与 y 是否共轭，若不共轭，则 $sign(M)$不是一个合法签名，验证失败；若共轭，则执行步骤 23;

步骤23、利用已获取的S的公钥计算$sign(M)x'$和xy，并判定二者是否共轭，若不共轭，则$sign(M)$不是一个合法签名，验证失败；若共轭，则$sign(M)$为消息M的合法签名。

其中，步骤 20 中获取 S 的公钥的方式为带外方式，或者该公钥由签名方 S 直接发送给验证方 V。

在所述步骤 22 中判定 $sign(M)$ 与 y 是否共轭和步骤 23 中判定 $sign(M)x'$ 和 xy 是否共轭采用算法 $BCDA$。该算法 $BCDA$ 如图 5 所示：

任何一个非交换群，都存在一个从群到一个环的函数，该函数对于共轭对的函数值相等，把该函数叫做特征。定义一个从 $B_n(l)$到$Laurent$多项式环$Z[t, t^{-1}]$的一个函数：$g\rightarrow det(\Phi(g)-I)$，其中$g\in B_n(l)$，$\Phi(g)$为$g$的$Burau$表示，$I$

为单位矩阵，*det()*为求行列式的符号，显然该函数为$B_n(l)$的特征。把$det(\Phi(g)-I)$叫做辫元*g*的亚历山大多项式，记做$P_g(t)$，显然对于一个$g\in B_n(l)$，它的亚历山大多项式$P_g(t)$的秩$\partial(P_g(t)) \le l(n-1)n/2$。判断两个辫元*a*，$b\in B_n(l)$是否共轭，做如下的亚历山大测试：选定系统参数素数*p*和正整数*r*，在有限域*Z/pZ*上任意选取*r*个不相等的值t_1，t_2 … t_r，若对于所有的t_i（$i=1, 2 \cdots r$）都有$P_a(t_i)=P_b(t_i)$，则输出1，否则输出0。由于$\partial(P_a(t)-P_b(t)) \le l(n-1)n/2$，所以方程$P_a(t)-P_b(t)=0$最多只有$l(n-1)n/2$个根。所以概率$Pr[P_a(t)\neq P_b(t)|$亚历山大测试输出为*1*$] \le \left(\frac{l(n-1)n}{2p}\right)^r$显然随着p和r的增加，这个概率可以任意的小。亚历山大测试的计算复杂度为$O(rn^3)$。

*Maxinf-Minsup*测试。对于辫元的$x\in B_n(l)$，定义$Maxinf(x)=Max\{inf(y)|y\sim x, y\in B_n(l)\}$，$Minsup(x)=Min\{sup(y)|y\sim x, y\in B_n(l)\}$。所谓*Maxinf-Minsup*测试，即对辫元*a*，$b\in B_n(l)$，判断$Maxinf(a)=Maxinf(b)$，$Minsup(a)=Minsup(b)$是否都成立，若都成立，则输出1，否则输出0。下面给出计算*Maxinf(x)*和*Minsup*（*x*）的算法描述。首先定义两个操作，若$x=\Delta^u\pi_1\pi_2\cdots\pi_l$，$cycling(x)=(\tau^u(\pi_l))^{-1}x\,\tau^u(\pi_l)$，$decycling(x)=\pi_l^{-1}x\,\pi_l$。对x循环做*cycling*（*decycling*）操作，直到*inf*值增加（*sup*值减少），然后以当前得到的元素为新元素，重复该循环操作，且循环次数计数重新设置为1；若循环次数计数直到$m=n(n-1)/2$都*inf*值不再增加（*sup*值不再减少），则当前的元素的*inf*值即为*Maxinf(x)*(分别 *Minsup(x)*。该算法的理论分析请参看引文：*J. S. Birman, K. H. Ko and S. J. Lee, The in.mum, supremum and geodesic length of a braid conjugacy class, to appear in Advances in Mathematics.*。该算法的算法复杂度为$O(l^2 n\log n)$。

如果辫元*a*，*b*通过了亚历山大测试和*Maxinf-Minsup*测试，则可以判定$a\sim b$成立，只有一种例外情况，即$a\sim b^{-1}$。然而这对于随机选择的*a*、*b*来说，是几乎不可能出现的，而对于攻击者同样不能利用这种例外情况，分析见引文：*K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang and C. S. Park, New Public-Key Crytosystem Using Braid Groups, Proc. of Crypto 2000, LNCS 1880, Springer-Verlag (2000) 166 183*。

对于一个合法的签名*sign(M)*，由于$sign(M)=a^{-1}byb^{-1}a=(b^{-1}a)^{-1}yb^{-1}a$，故

$sign(M) \sim y$成立；而$x' sign(M) = a^{-1}xa\ a^{-1}byb^{-1}a = a^{-1}xbyb^{-1}a$，由于$x \in LB_m$，$b \in RB_{n-1-m}$，因此$xb = bx$，从而有$x' sign(M) = a^{-1}xa\ a^{-1}byb^{-1}a = a^{-1}xbyb^{-1}a = a^{-1}bxyb^{-1}a = (b^{-1}a)^{-1}(xy)(b^{-1}a)$，从而$x' sign(M) \sim xy$。因此一个合法的签名总是可以通过验证的。

本发明还提供一种既包括签名方又包括验证方的数字签名及其验证方法，参见图6，为本发明基于辫群共轭的数字签名及其验证方法，签名方对需要签名的消息M使用散列函数h得到$y=h(M) \in B_n(l)$，并产生密钥，随机生成一个辫元$b \in RB_{n-1-m}(l)$，签名方使用自己的私钥a和产生的随机辫元b对消息M签名得到$Sign(M) = a^{-1}byb^{-1}a$后，将消息$M$以及$M$的签名$Sign(M)$发送给验证方，验证方通过散列函数$h$对消息$M$进行计算得到$y=h(M)$及密钥中的公钥验证签名消息$M$，具体过程如下：

步骤1、签名方S选择三个辫元$x \in LBm(l)$，$x' \in B_n(l)$，$a \in B_n(l)$，使得他们满足$x' = a^{-1}xa$，且已知x和x'要找到a在计算上是不可行的，并将辫元对(x', x)作为S的公钥，辫元a作为S的私钥；

步骤2、签名方S对需要签名的消息M使用散列函数h得到$y=h(M) \in B_n(l)$；

步骤3、随机生成一个辫元$b \in RB_{n-1-m}(l)$，然后使用自己的私钥a和产生的随机辫元b对消息M签名得到$Sign(M) = a^{-1}byb^{-1}a$；

步骤4、签名方S将消息M以及M的签名$Sign(M)$发送给签名验证方V；

步骤5、签名验证方V接收签名方S发送的信息M以及M的签名$Sign(M)$后，获取S的公钥；

步骤6、利用系统参数散列函数h对消息M进行计算，得到$y=h(M)$；

步骤7、判定$sign(M)$与y是否共轭，若不共轭，则$sign(M)$不是一个合法签名，验证失败；若共轭，则执行步骤8；

步骤8、利用已获取的S的公钥计算$sign(M)\ x'$和xy，并判定二者是否共轭，若不共轭，则$sign(M)$不是一个合法签名，验证失败；若共轭，则$sign(M)$为消息M的合法签名。

由于辫群是无限群，为了用计算机实现，需要设置系统参数。首先设定系统参数n，l，d（推荐l=3，d=4）。令$B_n(l) = \{b \in B_n \mid 0 \le inf(b),\ sup(b) \le l\}$，则$|B_n(l)| < (n!)^l$为有限的。同理$LB_m(l) = \{b \in LB_m \mid 0 \le inf(b),\ sup(b)$

$\leq l\}$，$RB_{n-1-m}(l) = \{b \in RB_{n-1-m} \mid 0 \leq inf(b),\ sup(b) \leq l\}$。对于一个辫元采用目前已知在计算机上计算速度最快的*Burau*表示，即用一个*Laurent*多项式环$Z[t, t^{-1}]$上的$(n-1) \times (n-1)$阶矩阵来表示，具体替换原则如下：

做如下的替换：

$$\sigma_1 = \begin{bmatrix} -t & & & \\ 1 & 1 & & \\ & \ddots & \ddots & \\ & & & 1 \end{bmatrix} \quad \sigma_2 = \begin{bmatrix} 1 & t & & \\ & -t & & \\ & 1 & 1 & \\ & & \ddots & 1 \end{bmatrix} \quad \cdots \quad \sigma_i = \begin{bmatrix} \ddots & & & \\ & 1 & t & \\ & & -t & \\ & & 1 & 1 \\ & & & \ddots \end{bmatrix}$$

$$\sigma_{n-1} = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & t \\ & & & -t \end{bmatrix}$$

一个属于$B_n(l)$辫元转化为一个*Burau*表示的计算复杂度为$O(ln)$，有了以上表示，与辫群内的群运算和求逆运算就转化为矩阵的乘法和求逆运算，他们都有着很有效的数学工具可以解决，它们的计算复杂度都为$O(ln)$。

本发明所述的方法可以用软件实现，为了提高速度，算法*BCDA*也可用硬件实现，其中，选定系统参数公开：辫群参数n，l，d，p(推荐n为20 ~ 30间，l=3，d=4，p为2^{31} ~ 2^{32}间)，以及左辫群大小m(推荐$n-m$为4左右)；选定用于散列消息的散列函数h；在签名方S的处理过程如下：

密钥产生：

1、使用算法*PBG*随机产生一个辫元$x \in LB_m$；

2、使用算法*RSSBG*(x, d)得到公钥（x'，x）和私钥a。

签名过程如下：

1、对需要签名的消息M应用散列函数h得到$y=h(M)$；

2、随机产生一个辫元b，然后计算byb^{-1}；

3、使用私钥，计算签名$sign(M) = a^{-1}byb^{-1}a$。

验证方V的处理过程如下：

1、对需要验证签名的消息M应用散列函数h得到$y=h(M)$；

2、使用算法*BCDA*判定$sign(M) \sim y$是否成立，若不成立，则验证失败，

结束；若成立，转步骤3；

3、计算$x'sign(M)$和xy；使用算法$BCDA$判定$x'sign(M)\sim xy$是否成立，若成立，则验证通过，结束，否则验证失败，结束。

最后应说明的是：以上实施例仅用以说明本发明而并非限制本发明所描述的技术方案；因此，尽管本说明书参照上述的各个实施例对本发明已进行了详细的说明，但是，本领域的普通技术人员应当理解，仍然可以对本发明进行修改或者等同替换；而一切不脱离本发明的精神和范围的技术方案及其改进，其均应涵盖在本发明的权利要求范围当中。

权利要求书

1、一种基于辫群共轭的数字签名方法，其特征在于，该方法涉及到的参数为：签名方（S），签名验证方（V），需要签名的消息（M），辫群生成元个数n，辫群左子群生成元个数m,辫元长度上界l,辫群$B_n(l)$，$B_n(l)$的左子群$LB_m(l)$，$Bn(l)$的右子群$RB_{n-1-m}(l)$，从比特串{0，1}*到辫群$Bn(l)$的单向散列函数h；所述签名方法包括以下步骤：

步骤1、签名方（S）选择三个辫元$x \in LB_m(l)$，$x' \in B_n(l)$，$a \in B_n(l)$，使得他们满足$x' = a^{-1}xa$，且已知x和x'要找到a在计算上是不可行的，并将辫元对(x', x)作为签名方（S）的公钥，辫元a作为签名方（S）的私钥；

步骤2、签名方（S）对需要签名的消息（M）使用散列函数h得到$y=h(M) \in B_n(l)$；

步骤3、随机生成一个辫元$b \in RB_{n-1-m}(l)$，然后使用自己的私钥a和产生的随机辫元b对消息（M）签名得到$Sign(M) = a^{-1}byb^{-1}a$；

步骤4、签名方（S）将消息（M）以及消息（M）的签名$Sign(M)$输出。

2、根据权利要求1所述的基于辫群共轭的数字签名方法，其特征在于，所述步骤1中签名方（S）的公钥辫元对(x', x)及私钥辫元a的生成具体包括以下步骤：

步骤 1a、选定系统参数辫群公钥对间的距离 d;

步骤 1b、将辫元 x 表示为标准形式 $x=\Delta^u \pi_1 \pi_2 \cdots \pi_l$;

步骤 1c、随机选择一个辫元 b 属于集合 $B_n(5\ l)$;

步骤 1d、计算 $x'=b^{-1}xb, a=b$;

步骤 1e、随机产生一个比特，若为 1，则计算 $x' = decycling(x'), a = a\ \pi_l$; 若不为 1，计算 $x'=cycling(x')$，$a = a\ \tau^u(\pi_l)$;

步骤1f、判断x'是否属于集合$SSS(x)$以及 $l(x') \leqslant d$是否都成立，若都成立输出辫元对（x, x'）作为公钥， a作为私钥；若有一个不成立，则执行步骤1e。

3、根据权利要求 1 所述的基于辫群共轭的数字签名方法，其特征在于，所述步骤 2 中使用散列函数 h 得到 $y=h(M) \in B_n(l)$的过程包括以下步骤：

步骤 2a、选择一个普通散列函数 H，其输出 $H(M)$长度为 $N = l[\log_2{}^{nl}]$，然

后将 $H(M)$一次等分为 l 段 $R_1||R_2||\ \cdots\ ||R_l$;

步骤 2b、依次将 Ri 对应为置换辫元 Ai，然后计算 $h(M)=A1*A2\cdots Al$ 即为所求的 $h(M)$。

4、根据权利要求 1 或 2 或 3 所述的基于辫群共轭的数字签名方法，其特征在于，所述的辫群生成元个数 n 的取值为 20 ~ 30，所述的辫元长度上界的值为 l=3，d=4，以及左子群大小 n-m =4。

5、一种基于辫群共轭的数字签名的验证方法，其特征在于，包括以下步骤:

步骤 1、签名验证方（V）接收签名方（S）发送的信息（M）以及信息（M）的签名 $Sign(M)$后，获取签名方（S）的公钥;

步骤 2、利用系统参数散列函数 h 对消息（M）进行计算，得到 $y=h(M)$;

步骤 3、判定 $sign(M)$ 与 y 是否共轭，若不共轭，则 $sign(M)$不是一个合法签名，验证失败；若共轭，则执行步骤 4;

步骤 4、利用已获取的 S 的公钥计算 $sign(M)$ x' 和 xy，并判定二者是否共轭，若不共轭，则 $sign(M)$不是一个合法签名，验证失败；若共轭，则 $sign(M)$为消息（M）的合法签名。

6、根据权利要求 5 所述的对基于辫群共轭的数字签名的验证方法，其特征在于，所述步骤 1 中获取签名方（S）的公钥的方式为带外方式或接收由签名方（S）发送的方式。

7、根据权利要求 5 所述的对基于辫群共轭的数字签名的验证方法，其特征在于，所述步骤 3 中判定 $sign(M)$ 与 y 是否共轭和步骤 4 中判定 $sign(M)$ x' 和 xy 是否共轭采用算法 $BCDA$。

8、一种基于辫群共轭的数字签名及其验证方法，其特征在于，该方法涉及到的参数为：签名方（S），签名验证方（V），需要签名的消息（M），辫群生成元个数n，辫群左子群生成元个数m,辫元长度上界l,辫群 $B_n(l)$，$B_n(l)$的左子群$LB_m(l)$，$B_n(l)$的右子群$RB_{n-l-m}(l)$，从比特串{0，1}*到辫群$B_n(l)$的单向散列函数h；所述签名方法包括以下步骤:

步骤1、签名方（S）选择三个辫元$x \in LB_m(l)$，$x' \in B_n(l)$，$a \in B_n(l)$，使得他们满足$x' = a^{-1}xa$，且已知x和x'要找到a在计算上是不可行的，并将辫元对

(x', x)作为签名方（S）的公钥，辫元a作为签名方（S）的私钥；

步骤2、签名方（S）对需要签名的消息（M）使用散列函数h得到$y=h(M) \in B_n(l)$；

步骤3、随机生成一个辫元$b \in RB_{n-1-m}(l)$，然后使用自己的私钥a和产生的随机辫元b对消息（M）签名得到$Sign(M)=a^{-1}byb^{-1}a$；

步骤4、签名方（S）将消息（M）以及消息（M）的签名$Sign(M)$输出给签名验证方（V）；

步骤5、签名验证方（V）接收签名方（S）发送的信息（M）以及消息（M）的签名$Sign(M)$后，获取签名方（S）的公钥；

步骤6、利用系统参数散列函数h对消息（M）进行计算，得到$y=h(M)$；

步骤7、判定$sign(M)$与y是否共轭，若不共轭，则$sign(M)$不是一个合法签名，验证失败；若共轭，则执行步骤8；

步骤8、利用已获取的签名方（S）的公钥计算$sign(M)$ x'和xy，并判定二者是否共轭，若不共轭，则$sign(M)$不是一个合法签名，验证失败；若共轭，则$sign(M)$为消息（M）的合法签名。

9、根据权利要求8所述的基于辫群共轭的数字签名及其验证方法，其特征在于，所述步骤1中签名方（S）的公钥辫元对(x', x)及私钥辫元a的生成包括如下步骤：

步骤1a、选定系统参数辫群公钥对间的距离d；

步骤1b、将辫元x表示为标准形式$x=\Delta^u\pi_1\pi_2\cdots\pi_l$；

步骤1c、随机选择一个辫元b属于集合$B_n(5l)$；

步骤1d、计算$x'=b^{-1}xb, a=b$；

步骤1e、随机产生一个比特，若为1，则计算$x'=decycling(x'), a=a\pi_l$；若不为1，计算$x'=cycling(x')$，$a=a\tau^u(\pi_1)$；

步骤1f、判断x'是否属于集合$SSS(x)$以及$l(x') \leqslant d$是否都成立，若都成立输出（x, x'）作为公钥，a作为私钥；若有一个不成立，则执行步骤1e。

10、根据权利要求8所述的基于辫群共轭的数字签名及其验证方法，其特征在于，所述步骤2中使用散列函数h得到$y=h(M) \in B_n(l)$的过程包括以下步骤：

步骤 2a、选择一个普通散列函数 H，其输出 $H(M)$长度为 $N=l[log_2{}^{n!}]$，然后将 $H(M)$一次等分为 l 段 $R_1||R_2||\ \cdots\ ||R_l$;

步骤 2b、依次将 Ri 对应为置换辫元 Ai，然后计算 $h(M)=A1*A2\cdots Al$ 即为所求的 $h(M)$。

11、根据权利要求 8 或 9 或 10 所述的基于辫群共轭的数字签名及其验证方法，其特征在于，所述的辫群生成元个数 n 的取值为 20 ~ 30，所述的辫元长度上界的值为 l=3，d=4，以及左子群大小 n-m =4。

12、根据权利要求 8 所述的基于辫群共轭的数字签名及其验证方法，其特征在于，所述步骤 7 中判定 $sign(M)$ 与 y 是否共轭和步骤 8 中判定 $sign(M)$ x' 和 xy 是否共轭采用算法 $BCDA$。

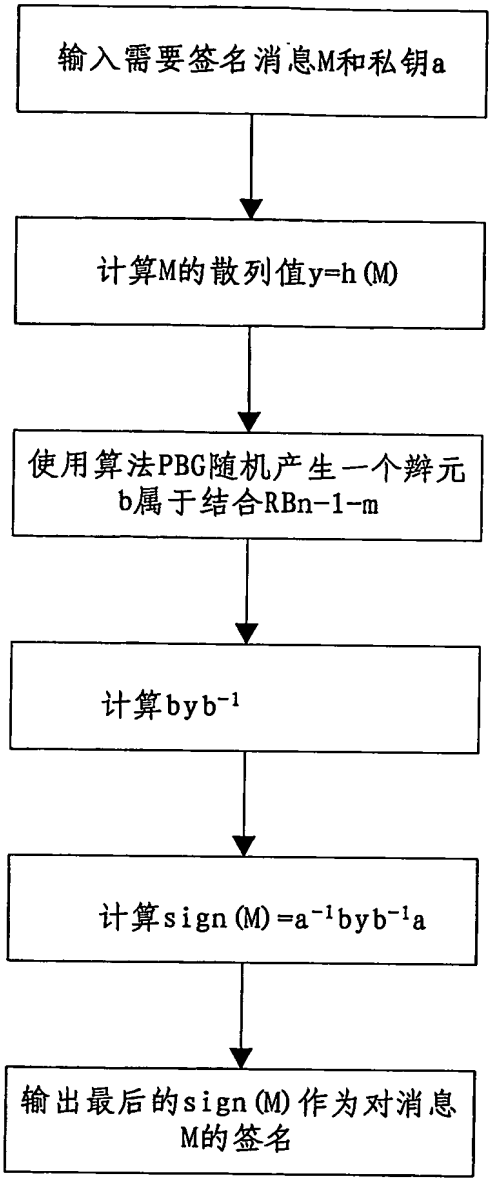
输入需要签名消息M和私钥a
计算M的散列值y=h(M)
使用算法PBG随机产生一个辫元b属于结合RBn-1-m
计算byb-1
计算sign(M)=a-1byb-1a
输出最后的sign(M)作为对消息M的签名

图 1

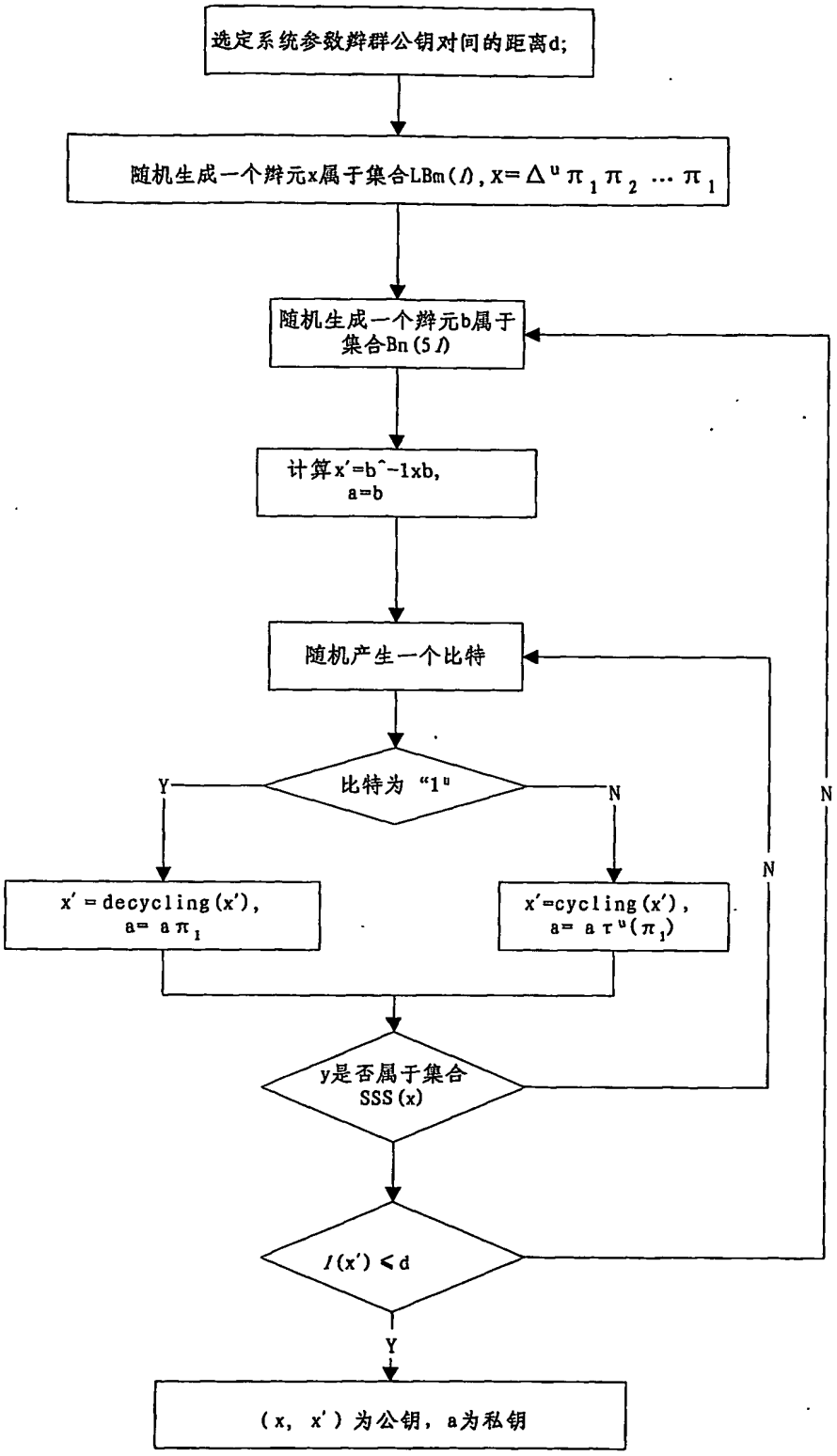
选定系统参数辫群公钥对间的距离d;
随机生成一个辫元x属于集合LBm(l), X=Δ^u π_1 π_2 … π_l
随机生成一个辫元b属于集合Bn(5l)
计算x'=b^-1xb, a=b
随机产生一个比特
比特为"1"
Y
N
x'=decycling(x'), a=aπ_1
x'=cycling(x'), a=aτ^u(π_1)
y是否属于集合SSS(x)
N
N
l(x')≤d
Y
(x, x')为公钥, a为私钥

图 2

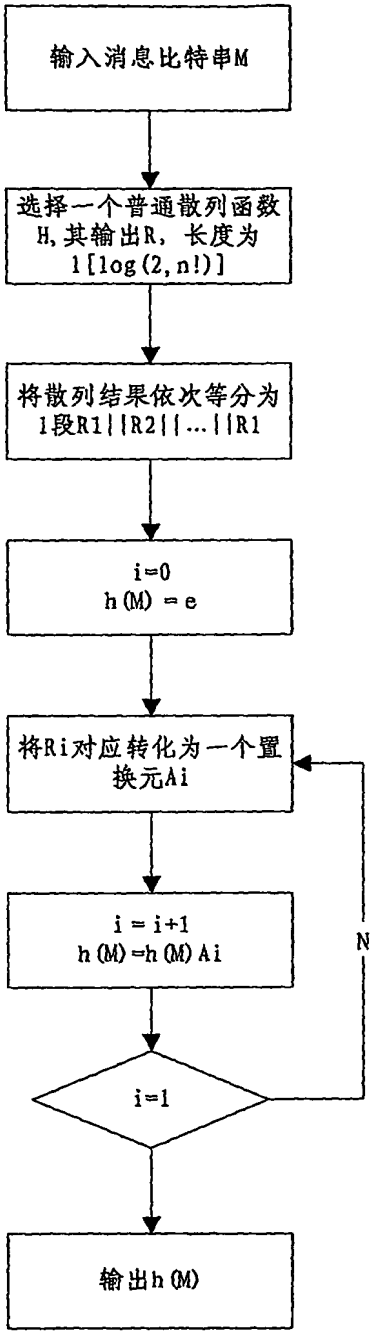
输入消息比特串M
选择一个普通散列函数H,其输出R，长度为l[log(2,n!)]
将散列结果依次等分为l段R1||R2||...||R1
i=0
h(M)=e
将Ri对应转化为一个置换元Ai
i=i+1
h(M)=h(M)Ai
i=l
N
输出h(M)

图 3

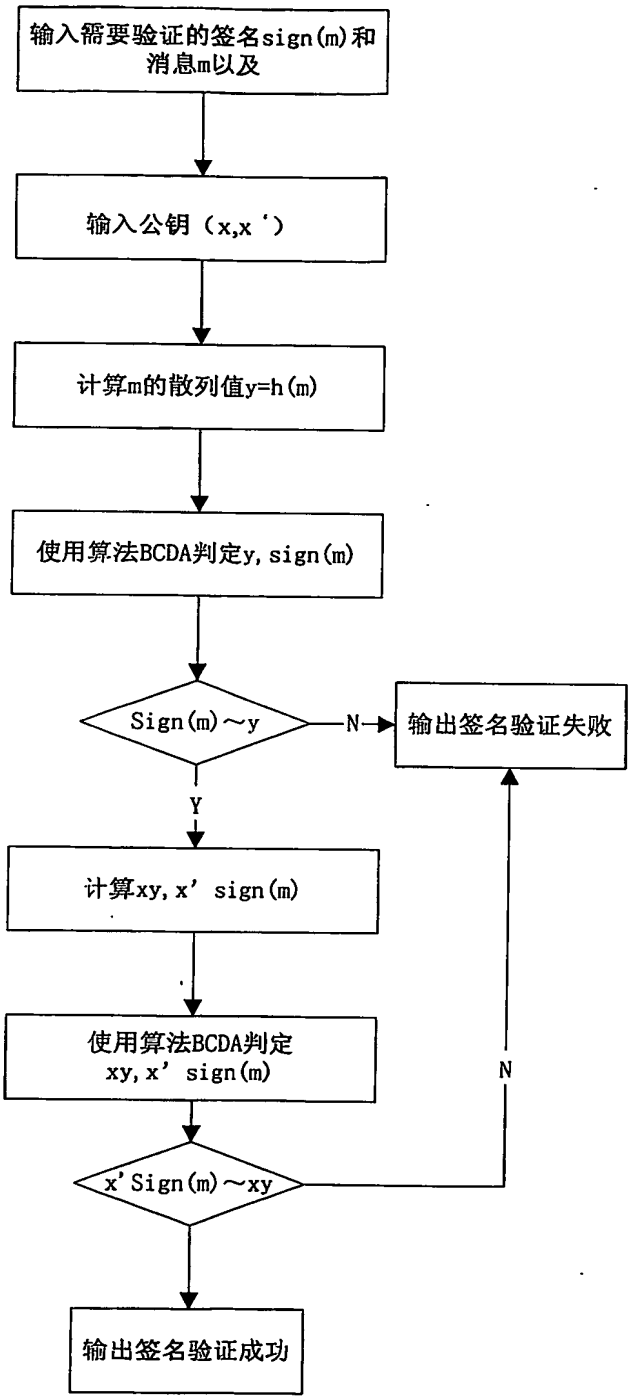
输入需要验证的签名sign(m)和消息m以及
输入公钥（x,x'）
计算m的散列值y=h(m)
使用算法BCDA判定y, sign(m)
Sign(m)～y
N
输出签名验证失败
Y
计算xy, x' sign(m)
使用算法BCDA判定 xy, x' sign(m)
N
x'Sign(m)～xy
输出签名验证成功

图 4

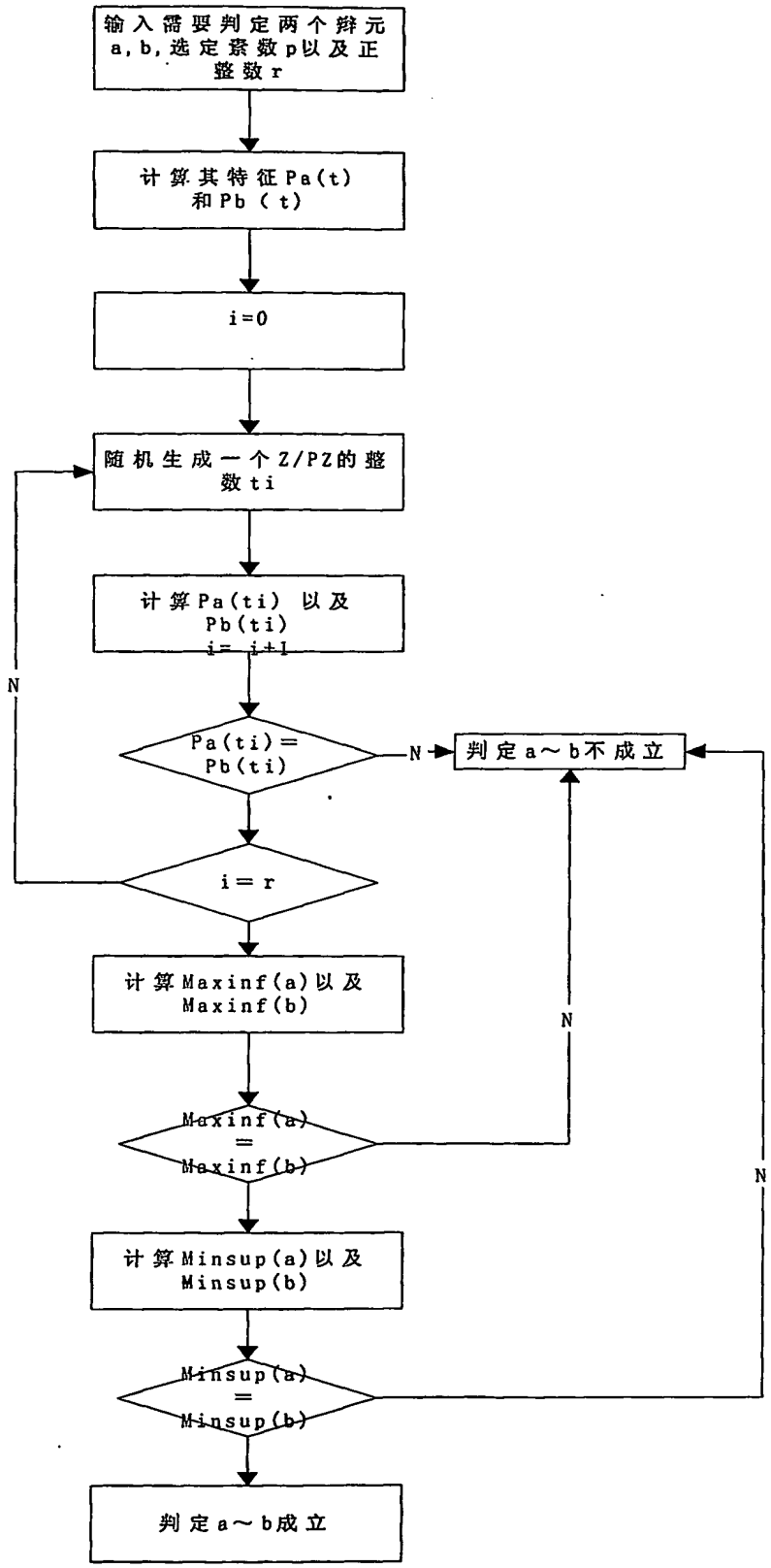
输入需要判定两个辩元a,b,选定素数p以及正整数r
计算其特征Pa(t)和Pb(t)
i=0
随机生成一个Z/PZ的整数ti
计算Pa(ti)以及Pb(ti)
i=i+1
Pa(ti)=Pb(ti)
N
判定a～b不成立
i=r
N
计算Maxinf(a)以及Maxinf(b)
Maxinf(a)=Maxinf(b)
N
计算Minsup(a)以及Minsup(b)
Minsup(a)=Minsup(b)
N
判定a～b成立

图 5

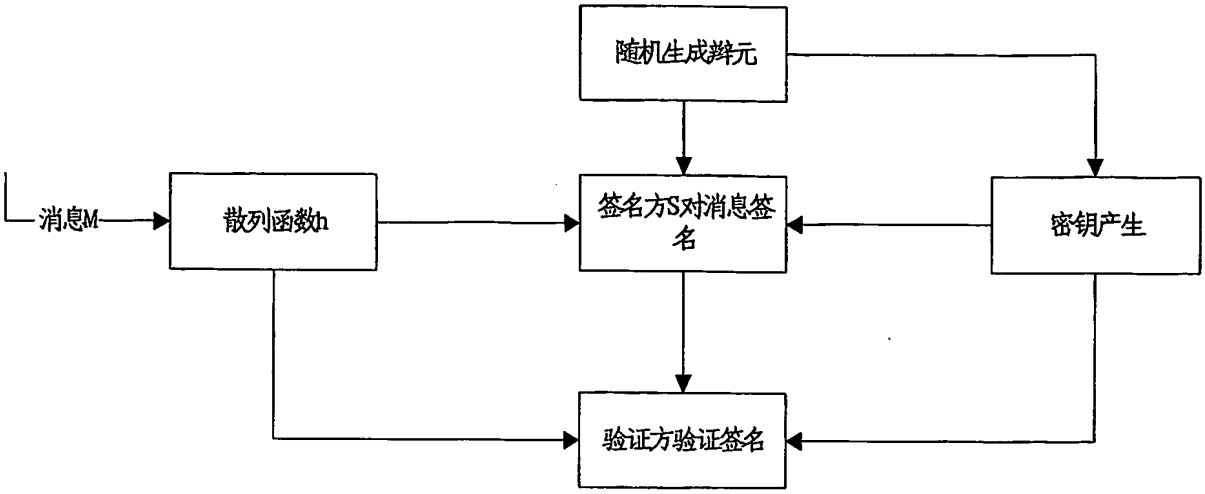

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2004/001289

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7 H04L9/30 H04L H04Q3 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT.EPODOC,WPI,PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO9944324A(ARITHMETICA,INC), 02.Sep.99(02.09.99)the whole document	1-12
A	WO03036863A(FRANCE TELECOM)1.May.03 (01.05.03), the whole document	1-12
A	WO03075582A(TELEFONAKTIEBOLAGET LM ERICSSON)12.Sep.03 (12.09.03), the whole document	1-12
A	CN1256463A(ZHAO F)14.Jun.00 (14.06.00), the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
26. Jan.05 (25.01.05)

Date of mailing of the international search report
17 FEB 2005 (17.02.2005)

Name and mailing address of the ISA/
6 Xitucheng Rd., Jimen Bridge, Haidian District,
100088 Beijing, China
Facsimile No. 86-10-62019451

Authorized officer
Leimin
Telephone No. (86-10)62084593

Form PCT/ISA /210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2004/001289

WO9944324A	02.09.99	AU759165B	10.04.03
		AU3180699A	15.09.99
		EP1074109A	07.02.01
		US2002001382A	03.01.02
		JP2002505550T	19.02.02
		US6493449B	10.12.02
CN1256463A	14.06.00	NONE	
WO03036863A	01.05.03	KR2004053209A	23.06.04
		FR2831738A	02.05.03
		EP1438804A	21.07.04
		AU2002358202A	06.05.03
WO03075582A	12.09.03	AU2002308241A	16.09.03

国际检索报告

国际申请号
PCT/CN2004/001289

A. 主题的分类

IPC7 H04L9/30

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类体系和分类号)

IPC7 H04L9/30 H04L H04Q3 G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称和，如果实际可行的，使用的检索词)

WPI, EPODOC, PAJ, CNPAT

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求编号
A	WO9944324A(ARITHMETICA,INC.)1999 年 9 月 2 日（02.09.99），摘要，说明书全文	1-12
A	WO03036863A(FRANCE TELECOM)2003 年 5 月 1 日（01.05.03），摘要，说明书全文	1-12
A	WO03075582A(TELEFONAKTIEBOLAGET LM ERICSSON)2003 年 9 月 12 日（12.09.03），摘要,说明书全文	1-12
A	CN1256463A(赵风光)2000 年 6 月 14 日（14.06.00），摘要，说明书全文	1-12

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的专用类型：

"A" 明确叙述了被认为不是特别相关的一般现有技术的文件

"E" 在国际申请日的当天或之后公布的在先的申请或专利

"L" 可能引起对优先权要求的怀疑的文件，为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布的在后文件，它与申请不相抵触，但是引用它是为了理解构成发明基础的理论或原理

"X" 特别相关的文件，仅仅考虑该文件，权利要求所记载的发明就不能认为是新颖的或不能认为是有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，权利要求记载的发明不具有创造性

"&" 同族专利成员的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2005 年 1 月 25 日（25.01.05）	17 · 2月 2005 (17 · 02 · 2005)
国际检索单位名称和邮寄地址 ISA/CN 中国北京市海淀区西土城路 6 号(100088) 传真号： 86-10-62019451	受权官员 雷敏 电话号码：86-10-62084593

国际检索报告
关于同族专利成员的情报

国际申请号
PCT/CN2004/001289

检索报告中引用的专利文件	公布日期	同族专利成员	公布日期
WO9944324A	02.09.99	AU759165B	10.04.03
		AU3180699A	15.09.99
		EP1074109A	07.02.01
		US6493449B	10.12.02
		JP2002505550T	19.02.02
		US2002001382A	03.01.02
CN1256463A	14.06.00	无	
WO03036863A	01.05.03	KR2004053209A	23.06.04
		FR2831738A	02.05.03
		EP1438804A	21.07.04
		AU2002358202A	06.05.03
WO03075582A	12.09.03	AU2002308241A	16.09.03